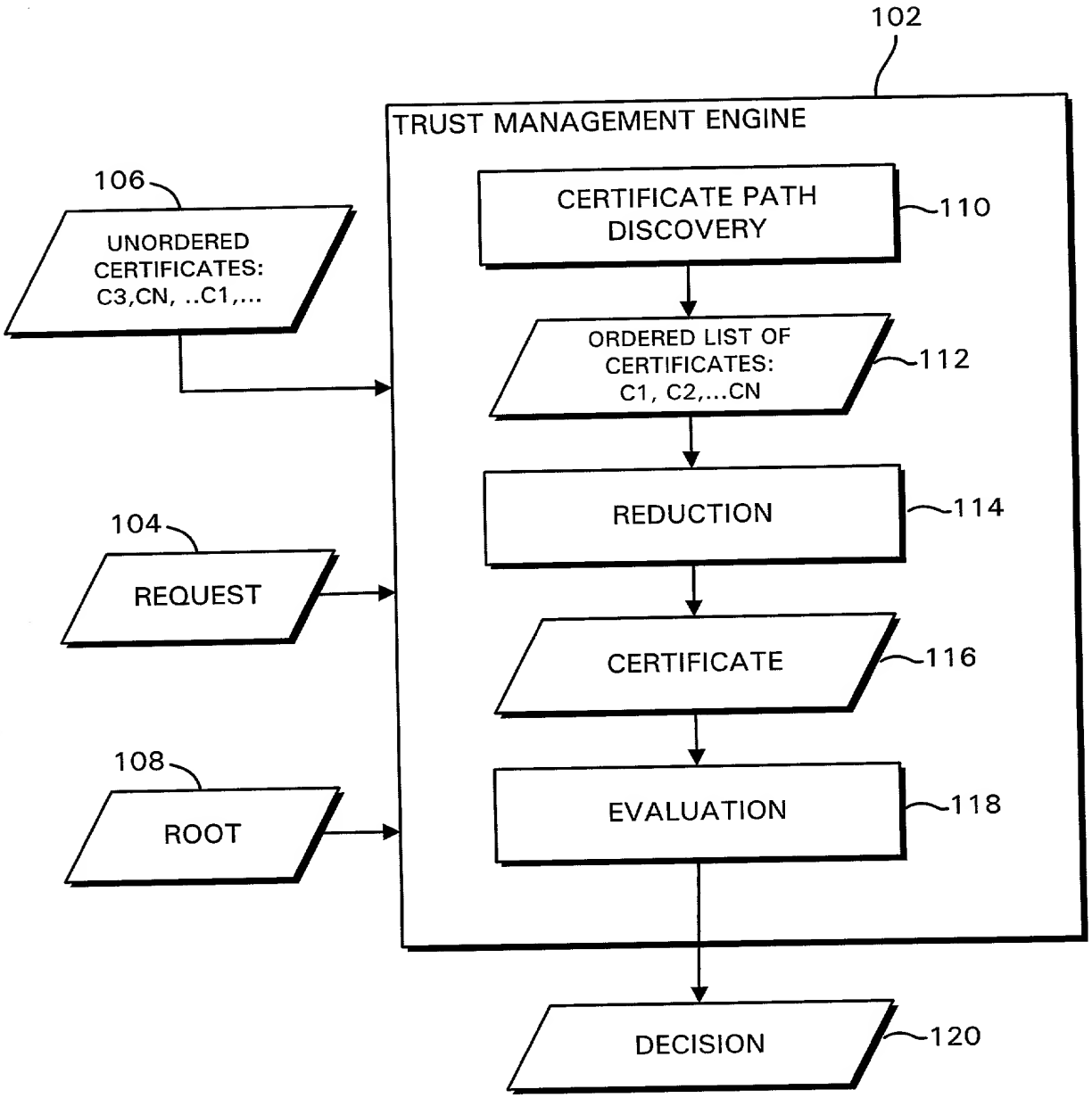

102
TRUST MANAGEMENT ENGINE
106
UNORDERED CERTIFICATES: C3,CN, ..C1,...
CERTIFICATE PATH DISCOVERY
110
ORDERED LIST OF CERTIFICATES: C1, C2,...CN
112
REDUCTION
114
104
REQUEST
CERTIFICATE
116
108
ROOT
EVALUATION
118
DECISION
120

FIG. 1

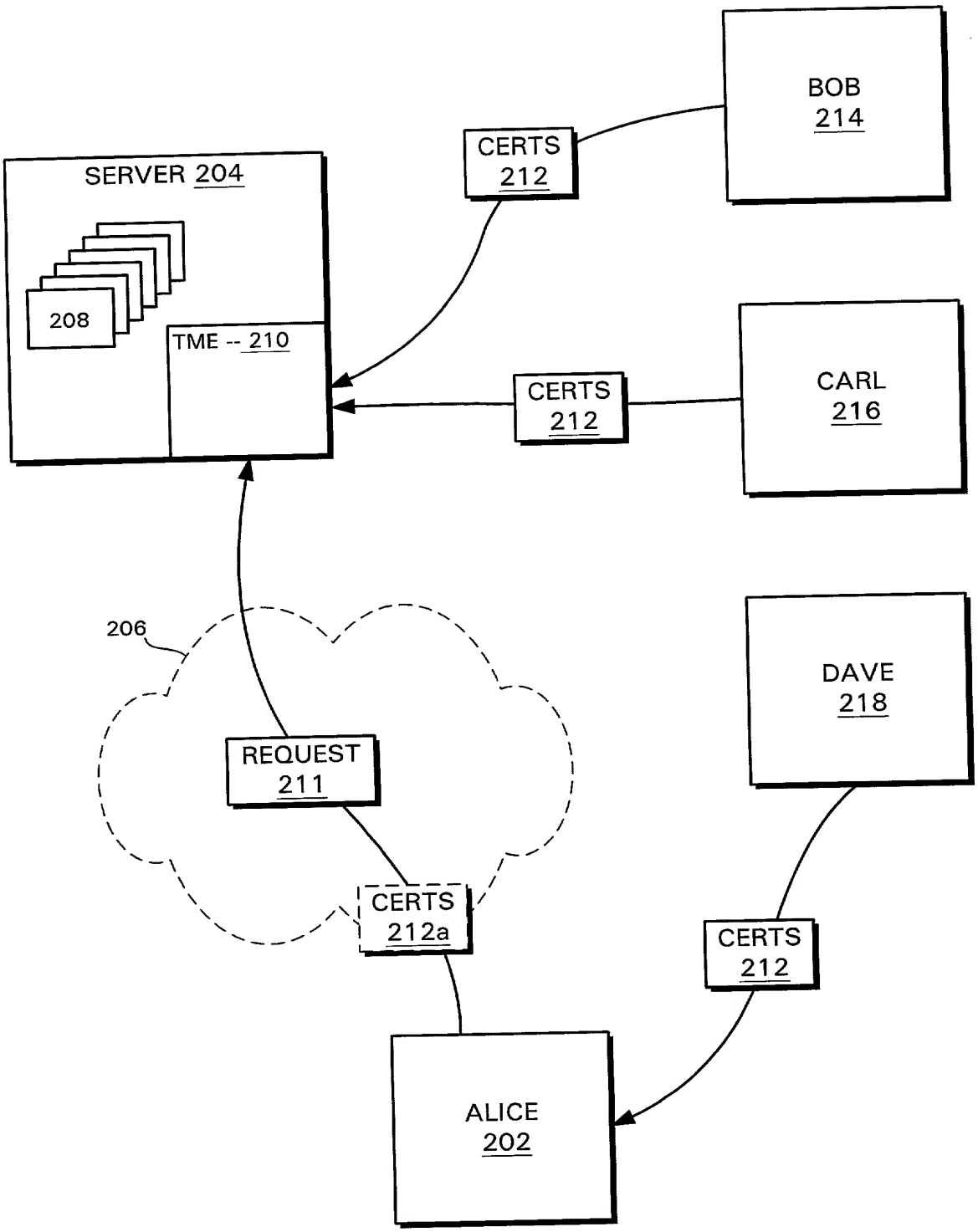


FIG. 2

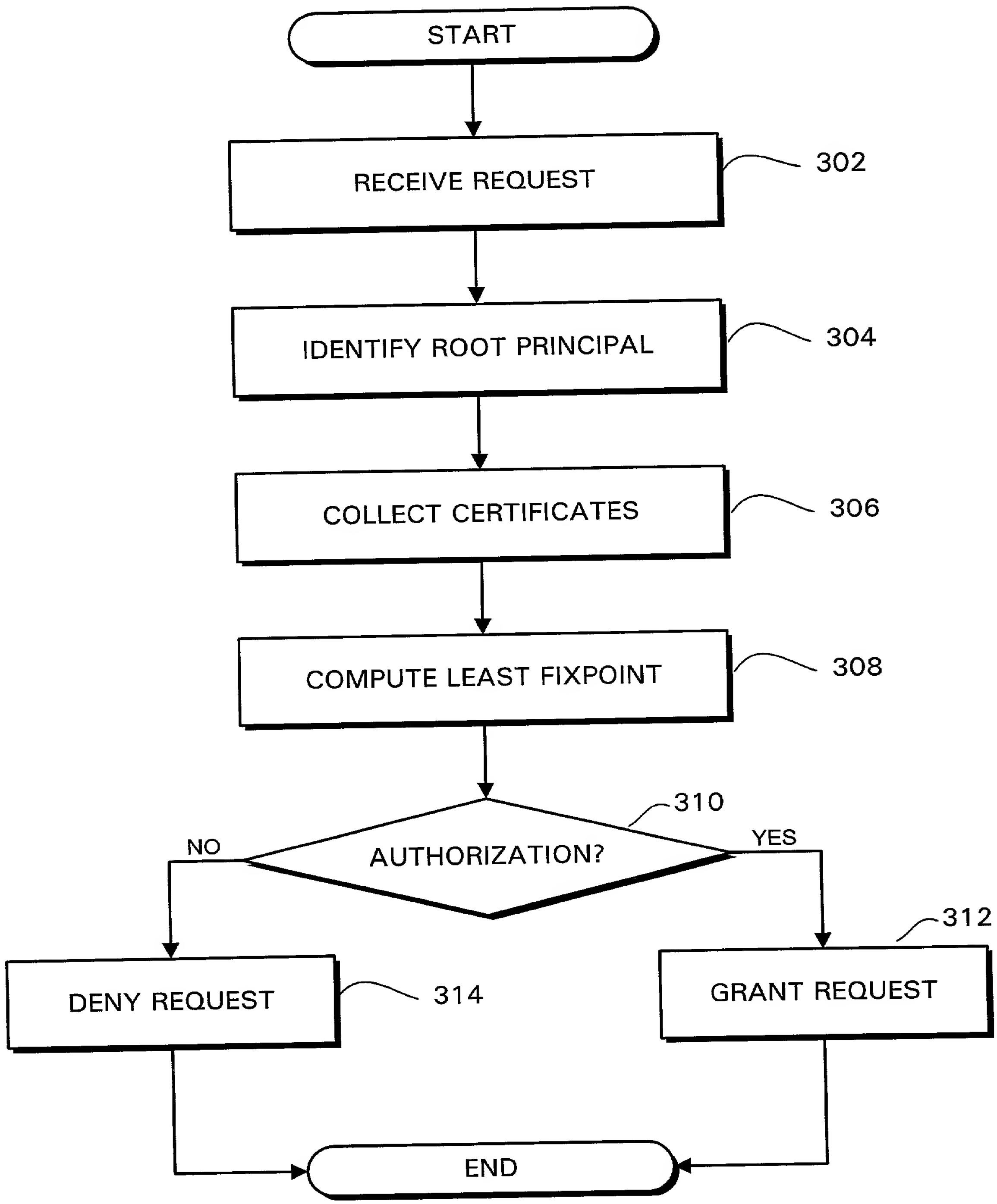

START
RECEIVE REQUEST
302
IDENTIFY ROOT PRINCIPAL
304
COLLECT CERTIFICATES
306
COMPUTE LEAST FIXPOINT
308
310
AUTHORIZATION?
NO
YES
312
DENY REQUEST
314
GRANT REQUEST
END

FIG. 3

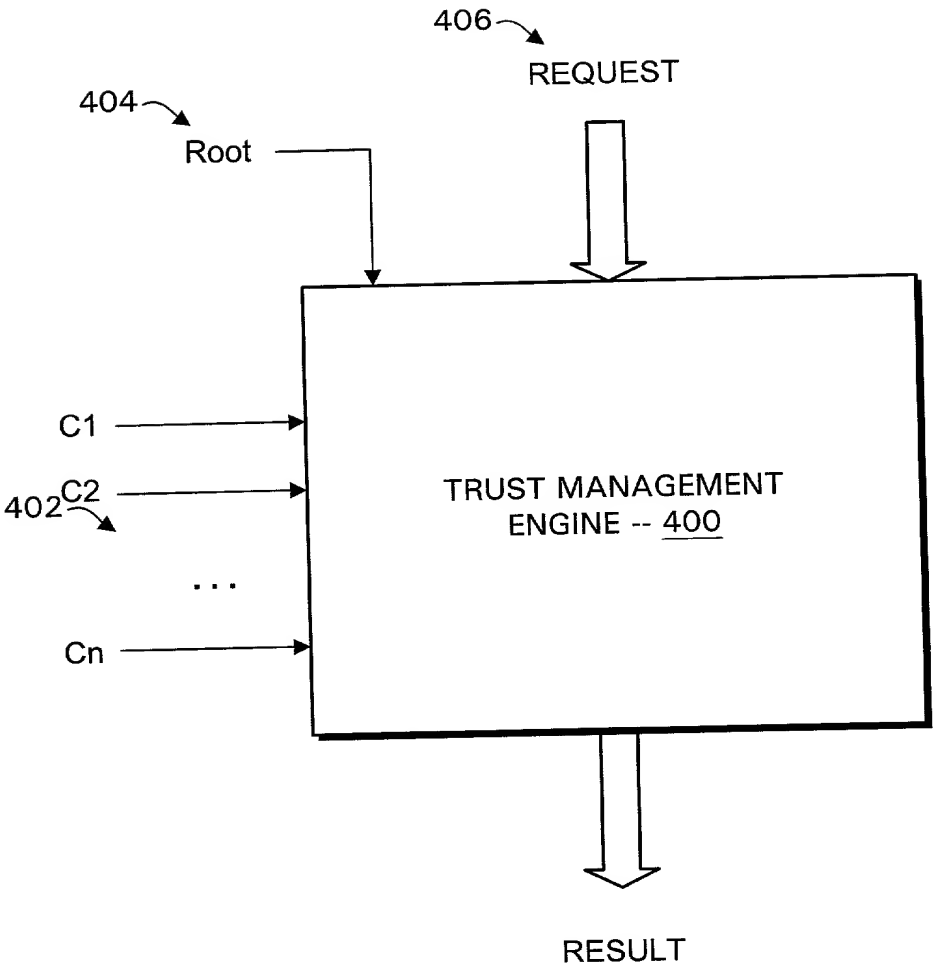

406
REQUEST
404
Root
C1
C2
402
...
Cn
TRUST MANAGEMENT
ENGINE -- 400
RESULT

FIG. 4

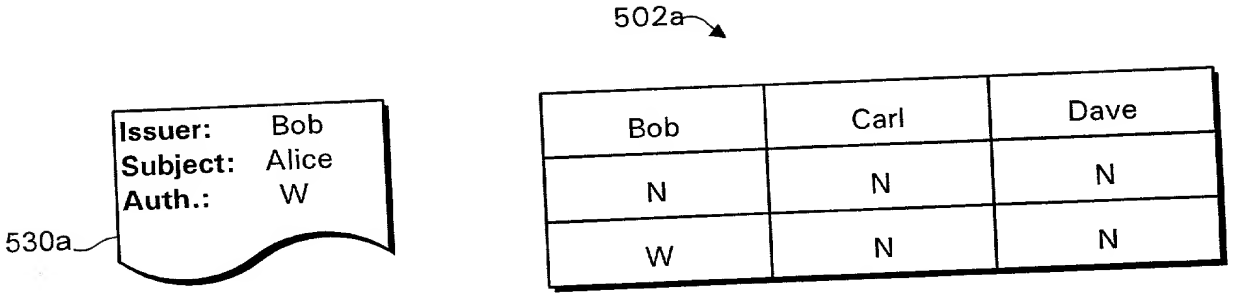


FIG. 5A

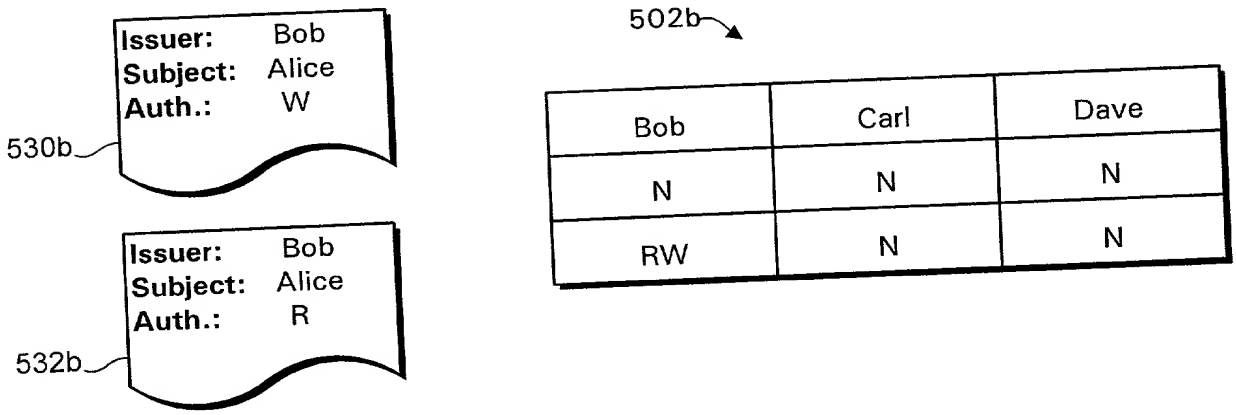
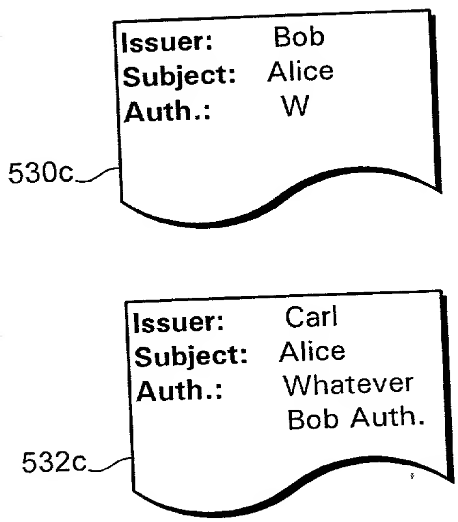


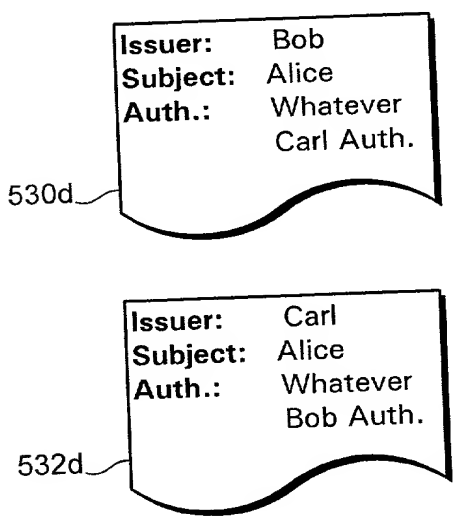
FIG. 5B



502c

Bob	Carl	Dave
N	N	N
W	N	N
W	W	N

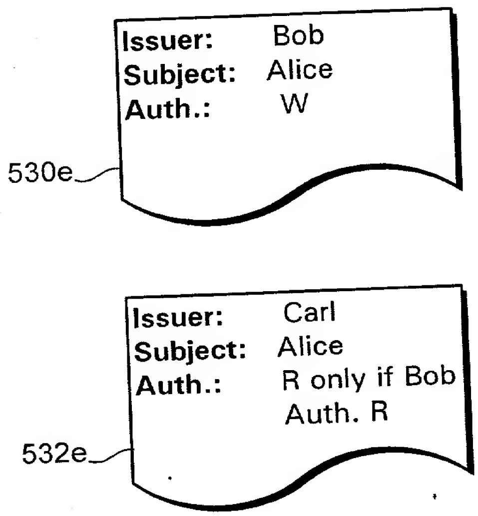
FIG. 5C



502d

Bob	Carl	Dave
N	N	N

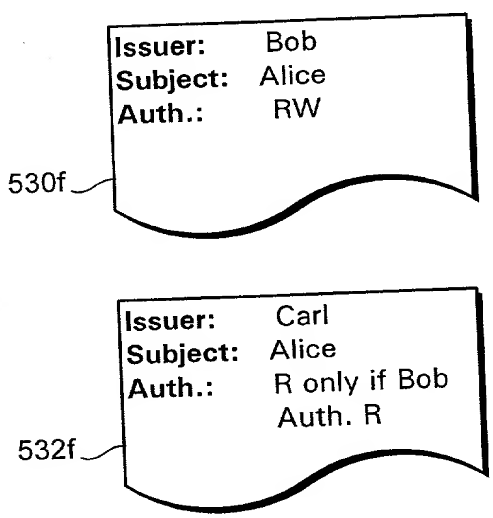
FIG. 5D



502e

Bob	Carl	Dave
N	N	N
W	N	N

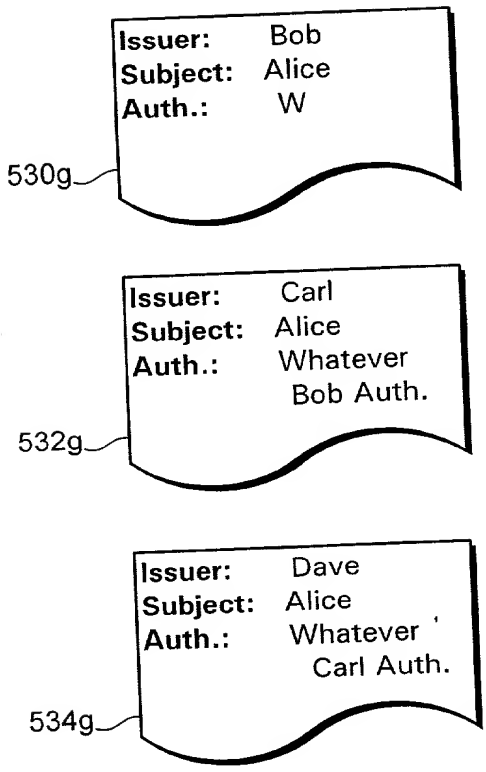
FIG. 5E



502f

Bob	Carl	Dave
N	N	N
RW	N	N
RW	R	N

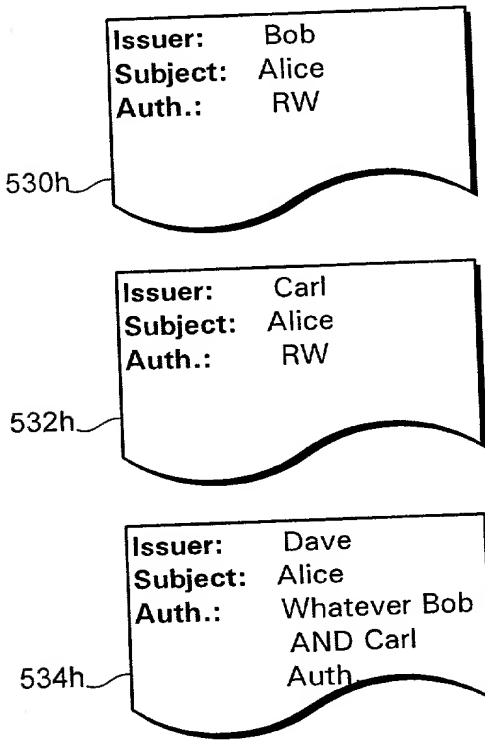
FIG. 5F



502g

Bob	Carl	Dave
N	N	N
W	N	N
W	W	N
W	W	W

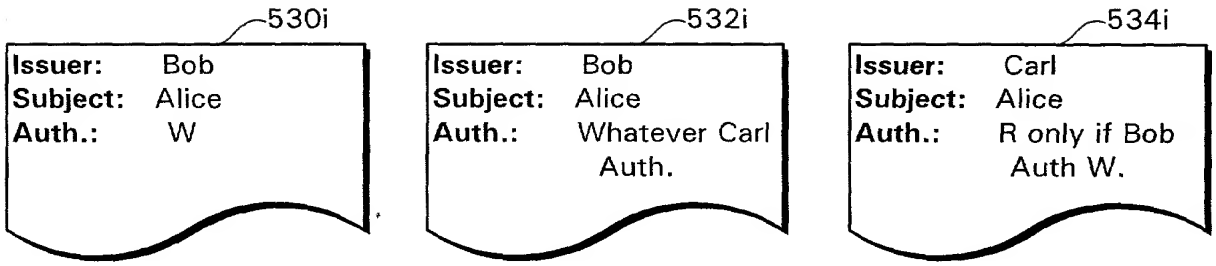
FIG. 5G



502h

Bob	Carl	Dave
N	N	N
W	RW	N
W	RW	W

FIG. 5H



502i

Bob	Carl	Dave
N	N	N
W	N	N
W	R	N
RW	R	N

FIG. 5I

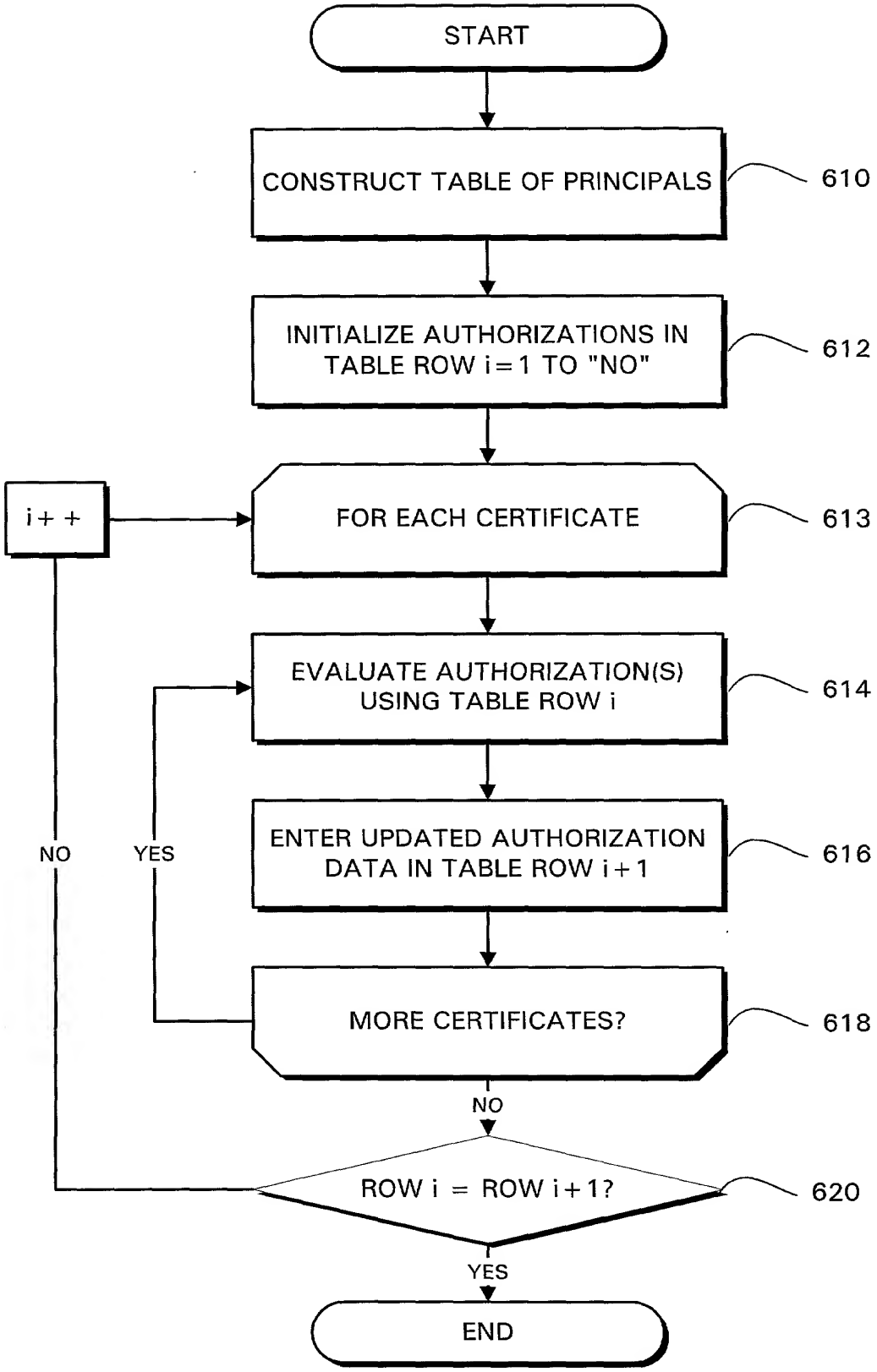

START
CONSTRUCT TABLE OF PRINCIPALS
610
INITIALIZE AUTHORIZATIONS IN TABLE ROW i = 1 TO "NO"
612
i++
FOR EACH CERTIFICATE
613
EVALUATE AUTHORIZATION(S) USING TABLE ROW i
614
ENTER UPDATED AUTHORIZATION DATA IN TABLE ROW i+1
616
MORE CERTIFICATES?
618
NO
YES
NO
ROW i = ROW i+1?
620
YES
END

FIG. 6

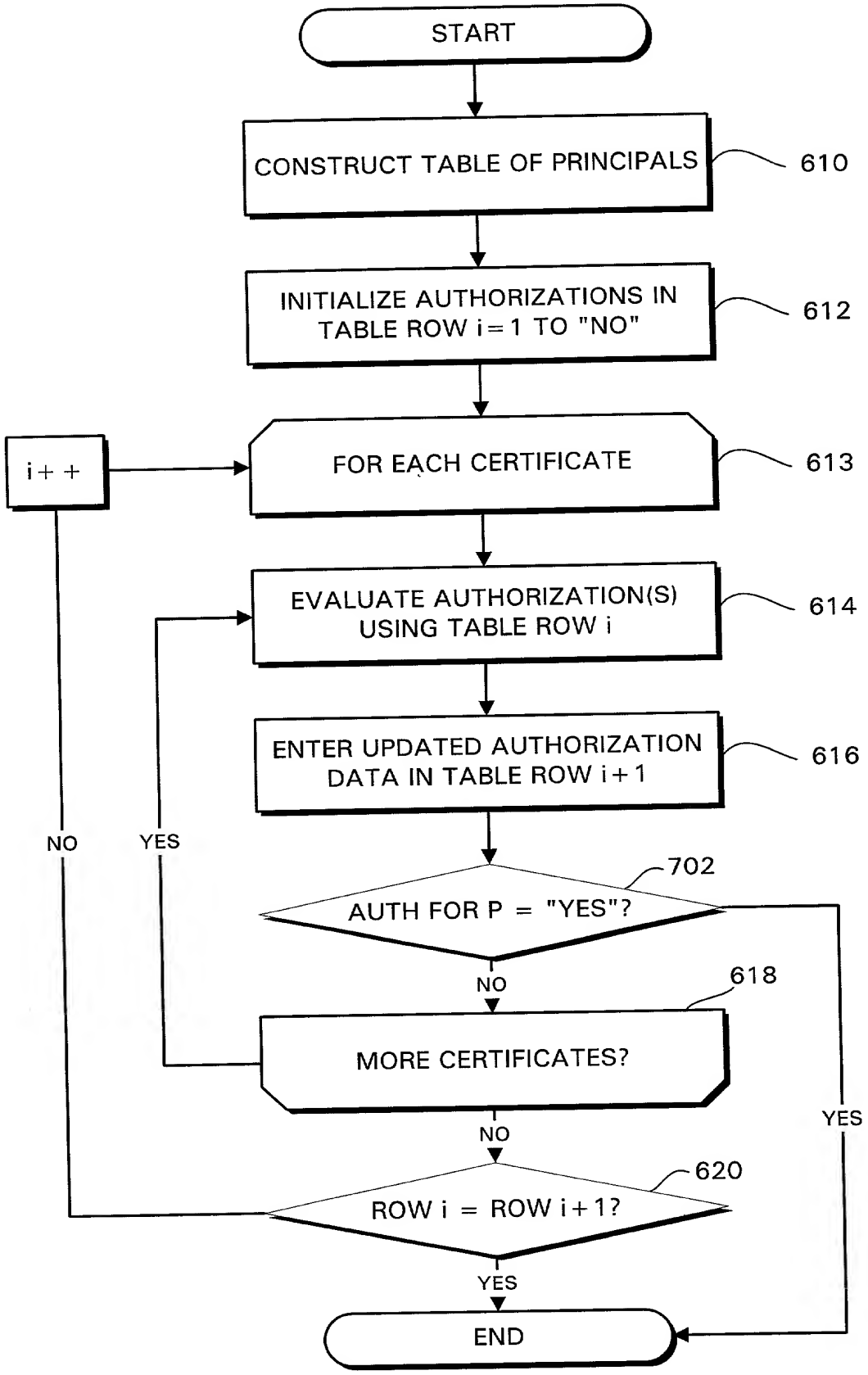

START
CONSTRUCT TABLE OF PRINCIPALS
610
INITIALIZE AUTHORIZATIONS IN TABLE ROW i=1 TO "NO"
612
i++
FOR EACH CERTIFICATE
613
EVALUATE AUTHORIZATION(S) USING TABLE ROW i
614
ENTER UPDATED AUTHORIZATION DATA IN TABLE ROW i+1
616
NO
YES
AUTH FOR P = "YES"?
702
NO
618
MORE CERTIFICATES?
YES
NO
ROW i = ROW i+1?
620
YES
END

FIG. 7

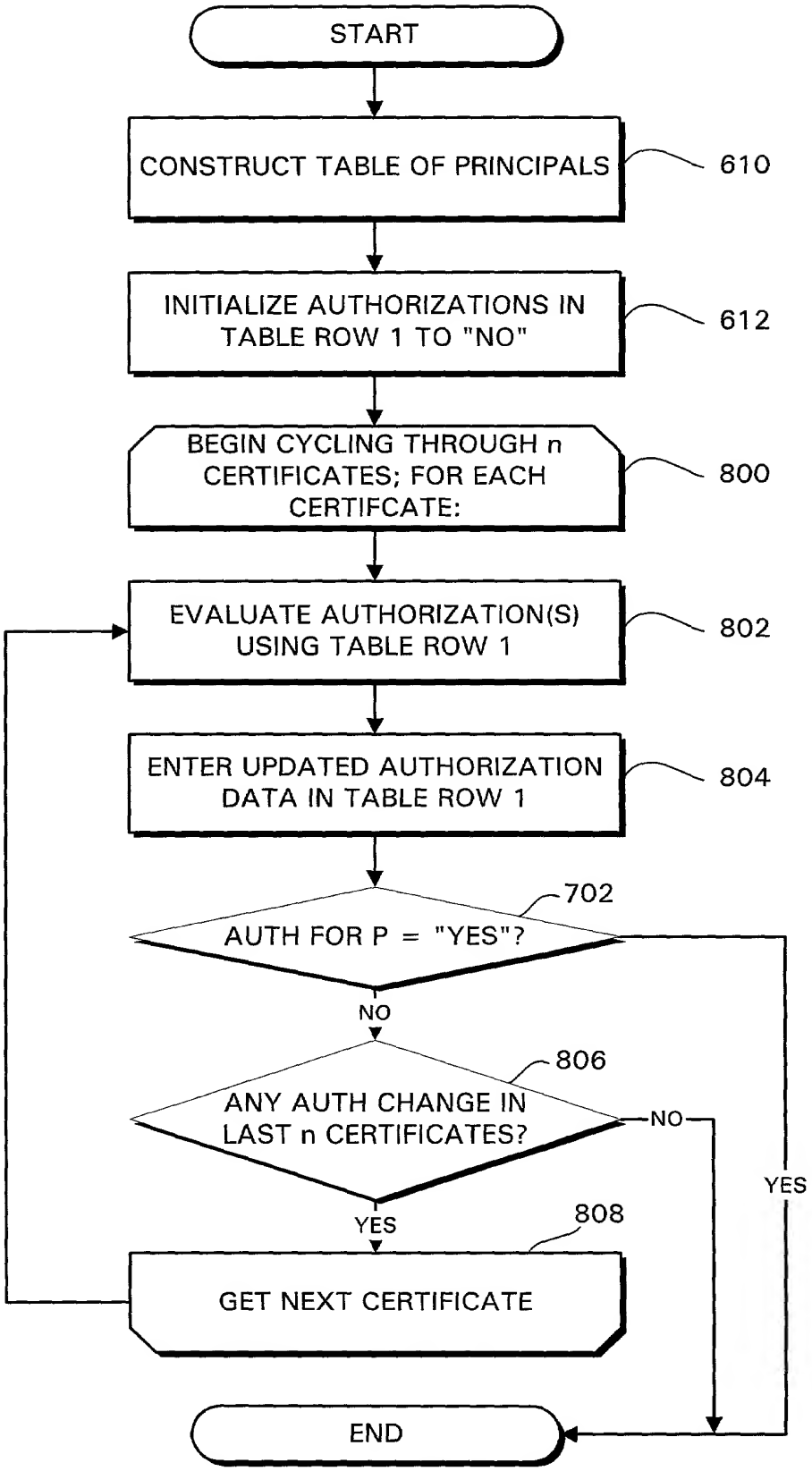

START
CONSTRUCT TABLE OF PRINCIPALS
610
INITIALIZE AUTHORIZATIONS IN TABLE ROW 1 TO "NO"
612
BEGIN CYCLING THROUGH n CERTIFICATES; FOR EACH CERTIFCATE:
800
EVALUATE AUTHORIZATION(S) USING TABLE ROW 1
802
ENTER UPDATED AUTHORIZATION DATA IN TABLE ROW 1
804
702
AUTH FOR P = "YES"?
NO
806
ANY AUTH CHANGE IN LAST n CERTIFICATES?
NO
YES
YES
808
GET NEXT CERTIFICATE
END

FIG. 8

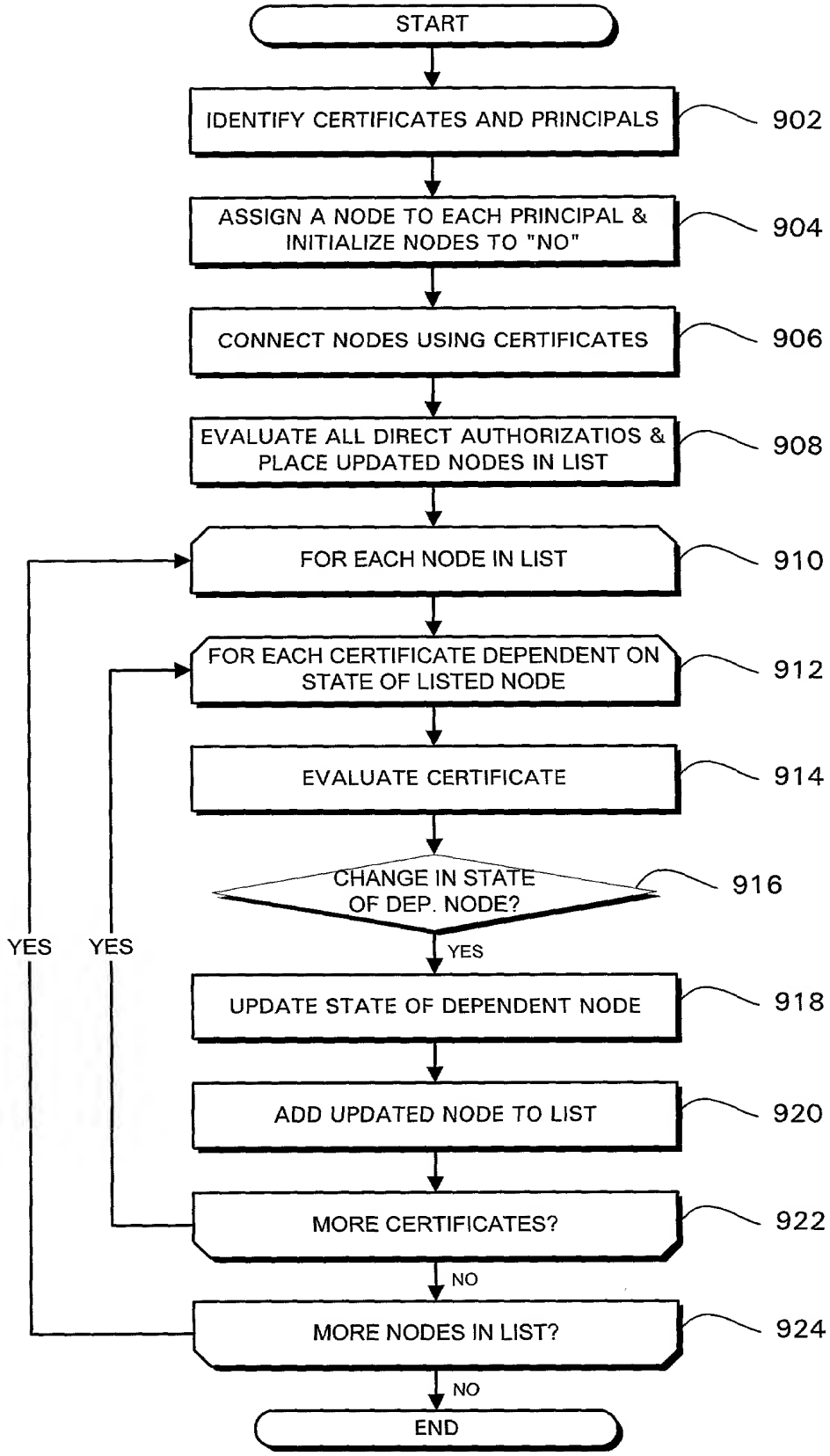

START
IDENTIFY CERTIFICATES AND PRINCIPALS
902
ASSIGN A NODE TO EACH PRINCIPAL & INITIALIZE NODES TO "NO"
904
CONNECT NODES USING CERTIFICATES
906
EVALUATE ALL DIRECT AUTHORIZATIOS & PLACE UPDATED NODES IN LIST
908
FOR EACH NODE IN LIST
910
FOR EACH CERTIFICATE DEPENDENT ON STATE OF LISTED NODE
912
EVALUATE CERTIFICATE
914
CHANGE IN STATE OF DEP. NODE?
916
YES
YES
YES
UPDATE STATE OF DEPENDENT NODE
918
ADD UPDATED NODE TO LIST
920
MORE CERTIFICATES?
922
NO
MORE NODES IN LIST?
924
NO
END

FIG. 9

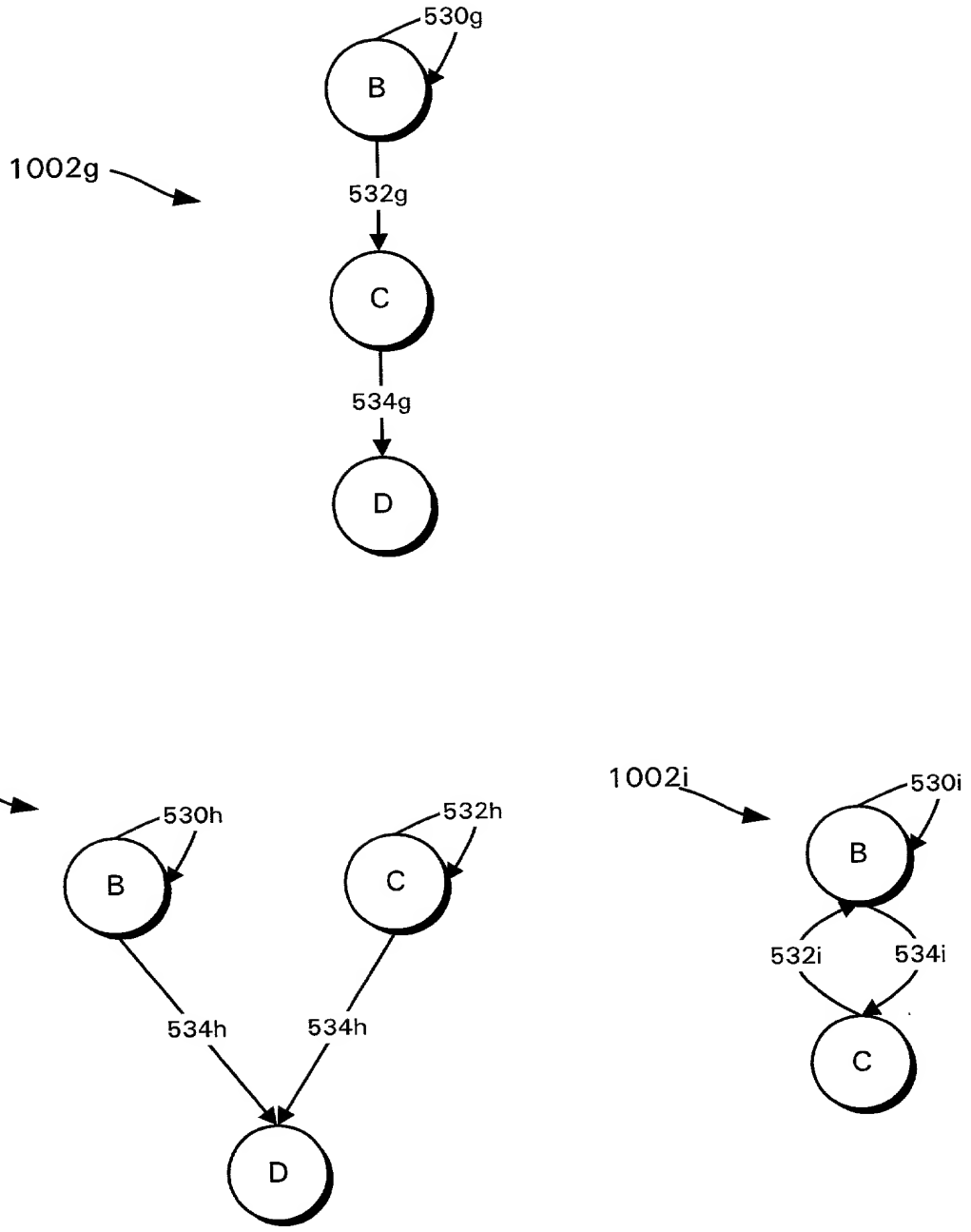

1002g
530g
B
532g
C
534g
D
1002h
530h
B
532h
C
534h
534h
D
1002i
530i
B
532i
534i
C

FIG. 10

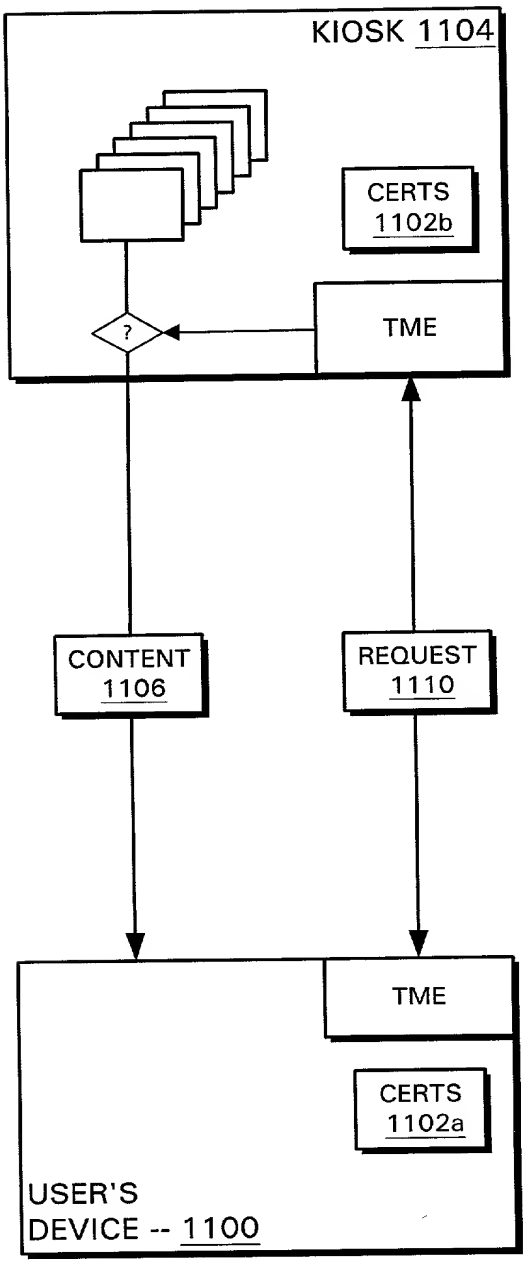

KIOSK 1104
CERTS
1102b
?
TME
CONTENT
1106
REQUEST
1110
TME
CERTS
1102a
USER'S
DEVICE -- 1100

FIG. 11

TABLE 1202 -- SPKI NAME ASSERTIONS

Issuer	Subject/Delegate	Name
Tech Corp.	Device No. 123	Music Player
Cert Corp.	Tech Corp.'s Music Player	Certified Device
Retail Store	Cert Corp.'s Certified Device	Supported Device

TABLE 1204 -- FIXPOINT COMPUTATION

Row	Tech Corp.'s Music Player	Cert Corp.'s Certified Device	Retail Store's Supported Device
1	{ }	{ }	{ }
2	{Device No. 123}	{ }	{ }
2	{Device No. 123}	{Device No. 123}	{ }
4	{Device No. 123}	{Device No. 123}	{Device No. 123}

FIG. 12

TABLE 1302 -- SPKI AUTHORIZATION ASSERTIONS

Issuer	Subject	Delegation	Authorization
Music Co.	DRM Co.	Yes	Download
DRM Co.	Retail Store	Yes	Download
Retail Store	Supported Device	No	Download

TABLE 1304 -- FIXPOINT COMPUTATION

Row	Music Co.	DRM Co.	Retail Store
1	No	No	No
2	No	No	Yes
2	No	Yes	Yes
4	Yes	Yes	Yes

FIG. 13

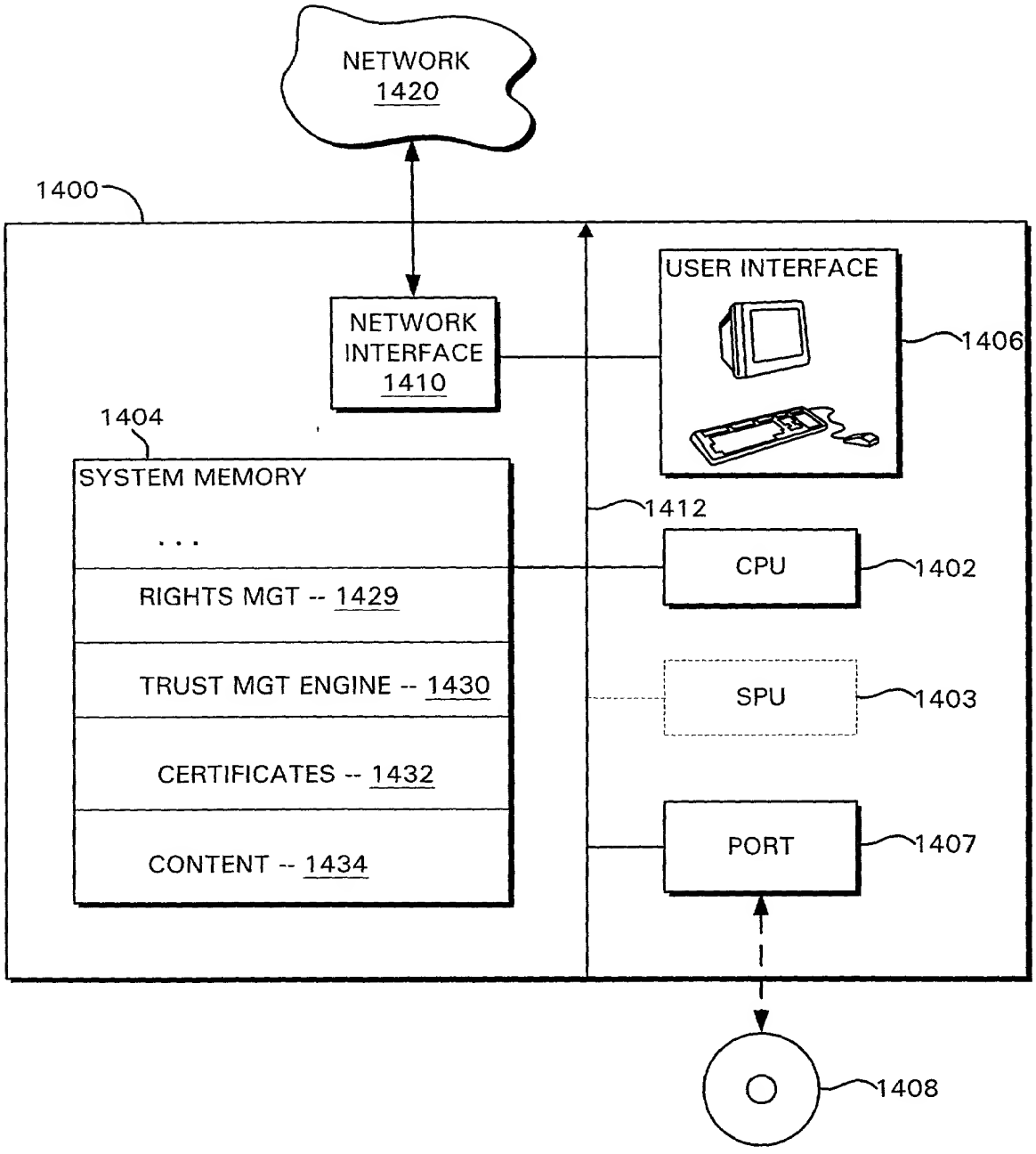

NETWORK
1420
1400
NETWORK
INTERFACE
1410
USER INTERFACE
1406
1404
SYSTEM MEMORY
. . .
RIGHTS MGT -- 1429
TRUST MGT ENGINE -- 1430
CERTIFICATES -- 1432
CONTENT -- 1434
1412
CPU
1402
SPU
1403
PORT
1407
1408

FIG. 14

$l \in License$	intended meaning
1) $\lambda m.\,\mathsf{W}$	Alice may write the file.
2) $\lambda m.\,m(\mathsf{Bob})$	Alice may do whatever Bob allows.
3) $\lambda m.\,\bigsqcup\{\mathsf{W}, m(\mathsf{Bob})\}$	Alice may write and do anything else Bob allows.
4) $\lambda m.\,\bigsqcap\{\mathsf{W}, m(\mathsf{Bob})\}$	Alice may write if Bob allows her to write.
5) $\lambda m.\,\bigsqcap\{\mathsf{W}, m(\mathsf{Bob}), m(\mathsf{Carl})\}$	Alice may write if both Bob and Carl say she can.
6) $\lambda m.$ if $card\{p \in \{\mathsf{Bob}, \mathsf{Carl}, \mathsf{Dave}\} \mid \mathsf{R} \sqsubseteq m(p)\} \geq 2$ then R else N	Alice may read if any two of Bob, Carl, and Dave say she can.
7) $\lambda m.$ if $\mathsf{W} \sqsubseteq m(\mathsf{Bob})$ then R else N	Alice may read if Bob says she may write.
8) $\lambda m.$ if $card\{p \mid \mathsf{R} \sqsubseteq m(p)\} \geq 2$ then R else N	Alice may read if any two principals say she can.

Figure 15. Example licenses

	$lfp(A)$ computation			
$A \in \mathcal{P}(Assertion)$	Bob	Carl	Dave	Comment
⟨Bob, $\lambda m.\,\mathsf{W}$⟩	N	N	N	A direct authorization.
	W	N	N	
⟨Bob, $\lambda m.\,\mathsf{W}$⟩	N	N	N	Auths combined using $\bigsqcup$.
⟨Bob, $\lambda m.\,\mathsf{R}$⟩	RW	N	N	
⟨Bob, $\lambda m.\,\mathsf{W}$⟩	N	N	N	Unconstrained delegation.
⟨Carl, $\lambda m.\,m(\mathsf{Bob})$⟩	W	N	N	
	W	W	N	
⟨Bob, $\lambda m.\,m(\mathsf{Carl})$⟩	N	N	N	Least fixpoint.
⟨Carl, $\lambda m.\,m(\mathsf{Bob})$⟩				
⟨Bob, $\lambda m.\,\mathsf{W}$⟩	N	N	N	Constrained delegation.
⟨Carl, $\lambda m.\,\bigsqcap\{\mathsf{R}, m(\mathsf{Bob})\}$⟩	W	N	N	
⟨Bob, $\lambda m.\,\mathsf{RW}$⟩	N	N	N	Constrained delegation.
⟨Carl, $\lambda m.\,\bigsqcap\{\mathsf{R}, m(\mathsf{Bob})\}$⟩	RW	N	N	
	RW	R	N	
⟨Bob, $\lambda m.\,\mathsf{W}$⟩	N	N	N	Chained delegation.
⟨Carl, $\lambda m.\,m(\mathsf{Bob})$⟩	W	N	N	
⟨Dave, $\lambda m.\,m(\mathsf{Carl})$⟩	W	W	N	
	W	W	W	
⟨Bob, $\lambda m.\,\mathsf{W}$⟩	N	N	N	Multiway delegation.
⟨Carl, $\lambda m.\,\mathsf{RW}$⟩	W	RW	N	
⟨Dave, $\lambda m.\,\bigsqcap\{m(\mathsf{Bob}), m(\mathsf{Carl})\}$⟩	W	RW	W	
⟨Bob, $\lambda m.\,\mathsf{W}$⟩	N	N	N	Inter-assertion communication.
⟨Bob, $\lambda m.\,m(\mathsf{Carl})$⟩	W	N	N	
⟨Carl, $\lambda m.$ if $\mathsf{W} \sqsubseteq m(\mathsf{Bob})$ then R else N⟩	W	R	N	
	RW	R	N	

Figure 16. Example least fixpoint computations of $\mathcal{M}_{Assertions}$

$$
\begin{array}{rcll}
p & \in & \mathit{Principal} & \\
u & \in & \mathit{Auth} & \\
m & \in & \mathit{AuthMap} & = \quad \mathit{Principal} \longrightarrow \mathit{Auth} \\
l & \in & \mathit{License} & = \quad \mathit{AuthMap} \longrightarrow_m \mathit{Auth} \\
a & \in & \mathit{Assertion} & = \quad \mathit{Principal} \times \mathit{License}
\end{array}
$$

$$
\mathcal{M}_{\mathit{Assertions}} : \mathcal{P}(\mathit{Assertion}) \longrightarrow_m \mathit{AuthMap}
$$

$$
\mathcal{M}_{\mathit{Assertions}}(A) = \mathit{lfp}(\lambda m.\lambda p. \bigsqcup \{ l(m) \mid \langle p, l \rangle \in A \})
$$

$$
\mathcal{M}_{\mathit{Engine}} : \mathit{Principal} \times \mathit{Auth} \times \mathcal{P}(\mathit{Assertion}) \longrightarrow \mathit{Bool}
$$

$$
\mathcal{M}_{\mathit{Engine}}(p, u, A) = u \sqsubseteq \mathcal{M}_{\mathit{Assertions}}(A)(p)
$$

Figure 17. Framework

$$
\begin{array}{rcll}
n & \in & \mathit{Name} & \\
y & \in & \mathit{Sexp} & \\
t & \in & \mathit{Time} & \\
u & \in & \mathit{Auth} & = \mathcal{P}(\mathit{Principal} \times (\mathit{Name} + \mathit{Sexp}) \times \mathit{Time}) \\
f & \in & \mathit{FullName} & = \mathit{Principal} \times \mathit{Name}^* \\
s & \in & \mathit{Subject} & = \mathit{FullName} + (\mathit{Int} \times \mathcal{P}(\mathit{FullName})) \\
d & \in & \mathit{Delegate} & = \mathit{Bool} \\
x & \in & \mathit{Action} & \\
 & & \mathit{TimePeriod} & = \mathit{Time} \times \mathit{Time} \\
 & & \mathit{NameAssertion} & = \mathit{Principal} \times \mathit{Name} \times \mathit{Subject} \times \mathit{TimePeriod} \\
 & & \mathit{AuthAssertion} & = \mathit{Principal} \times \mathit{Subject} \times \mathit{Delegate} \times \mathit{Action} \times \mathit{TimePeriod} \\
 & & \mathit{SPKIAssertion} & = \mathit{NameAssertion} + \mathit{AuthAssertion}
\end{array}
$$

$\mathcal{M}_{\mathit{Action}} : \mathit{Action} \longrightarrow \mathcal{P}(\mathit{Sexp})$ (omitted)

$\mathcal{M}_{\mathit{FullP}} : \mathit{FullName} \times \mathit{AuthMap} \longrightarrow \mathcal{P}(\mathit{Principal} \times \mathit{Time})$

$\mathcal{M}_{\mathit{FullP}}(\langle p, [] \rangle, m) = \{\langle p, t \rangle \mid t \in \mathit{Time}\}$

$$\mathcal{M}_{\mathit{FullP}}(\langle p, [n_0, n_1, \ldots] \rangle, m) = \left\{ \langle p', t \rangle \;\middle|\; \exists p''.\ \begin{array}{l} \langle p'', n_0, t \rangle \in m(p) \text{ and} \\ \langle p', t \rangle \in \mathcal{M}_{\mathit{FullP}}(\langle p'', [n_1, \ldots] \rangle, m) \end{array} \right\}$$

$\mathcal{M}_{\mathit{SubjP}} : \mathit{Subject} \times \mathit{AuthMap} \longrightarrow \mathcal{P}(\mathit{Principal} \times \mathit{Time})$

$\mathcal{M}_{\mathit{SubjP}}(f, m) = \mathcal{M}_{\mathit{FullP}}(f, m)$

$\mathcal{M}_{\mathit{SubjP}}(\langle k, F \rangle, m) = \{\langle p, t \rangle \mid k \leq \mathit{card}\{f \in F \mid \langle p, t \rangle \in \mathcal{M}_{\mathit{FullP}}(f, m)\}\}$

$\mathcal{M}_{\mathit{Name}} : \mathit{NameAssertion} \longrightarrow \mathit{Assertion}$

$\mathcal{M}_{\mathit{Name}}(p, n, s, \langle t_1, t_2 \rangle) = \langle p, \lambda m.\ \{\langle p', n, t \rangle \mid t_1 \leq t \leq t_2 \text{ and } \langle p', t \rangle \in \mathcal{M}_{\mathit{SubjP}}(s, m)\}\rangle$

$\mathcal{M}_{\mathit{FullA}} : \mathit{FullName} \times \mathit{AuthMap} \longrightarrow \mathit{Auth}$

$\mathcal{M}_{\mathit{FullA}}(f, m) = \{\langle p, y, t \rangle \mid \exists p'.\langle p', t \rangle \in \mathcal{M}_{\mathit{FullP}}(f, m) \text{ and } \langle p, y, t \rangle \in m(p')\}$

$\mathcal{M}_{\mathit{SubjA}} : \mathit{Subject} \times \mathit{AuthMap} \longrightarrow \mathit{Auth}$

$\mathcal{M}_{\mathit{SubjA}}(f, m) = \mathcal{M}_{\mathit{FullA}}(f, m)$

$\mathcal{M}_{\mathit{SubjA}}(\langle k, F \rangle, m) = \{\langle p, y, t \rangle \mid k \leq \mathit{card}\{f \in F \mid \langle p, y, t \rangle \in \mathcal{M}_{\mathit{FullA}}(f, m)\}\}$

$\mathcal{M}_{\mathit{Auth}} : \mathit{AuthAssertion} \longrightarrow \mathit{Assertion}$

$\mathcal{M}_{\mathit{Auth}}(p, s, d, x, \langle t_1, t_2 \rangle) = \langle p, l \rangle$, where

$$l(m) = \left\{ \langle p', y, t \rangle \;\middle|\; \begin{array}{l} y \in \mathcal{M}_{\mathit{Action}}(x) \text{ and } t_1 \leq t \leq t_2 \\ \text{and if } d \text{ then } \langle p', y, t \rangle \in \mathcal{M}_{\mathit{SubjA}}(s, m) \text{ else } \langle p', t \rangle \in \mathcal{M}_{\mathit{SubjP}}(s, m) \end{array} \right\}$$

Figure 18. SPKI instantiation

$$
\begin{array}{lcll}
v & \in & \mathit{Value} & \\
x & \in & \mathit{Action} & = \mathcal{P}(\mathit{String} \times \mathit{String}) \\
 & & \mathit{Request} & = \mathcal{P}(\mathit{Principal}) \times \mathit{Action} \\
u & \in & \mathit{Auth} & = \mathit{Request} \longrightarrow \mathit{Value} \\
z & \in & \mathit{Licensees} & \\
c & \in & \mathit{Conditions} & \\
 & & \mathit{KeyNoteAssertion} & = \mathit{Principal} \times \mathit{Licensees} \times \mathit{Conditions}
\end{array}
$$

$\mathcal{M}_{\mathit{Licensees}} : \mathit{Licensees} \times (\mathit{Principal} \longrightarrow \mathit{Value}) \longrightarrow_m \mathit{Value}$ (omitted)
$\mathcal{M}_{\mathit{Conditions}} : \mathit{Conditions} \times \mathit{Request} \longrightarrow \mathit{Value}$ (omitted)

$\mathcal{M}_{\mathit{Keynote}} : \mathit{KeyNoteAssertion} \longrightarrow \mathit{Assertion}$
$\mathcal{M}_{\mathit{Keynote}}(p, z, c) = \langle p, \lambda m.\, \lambda\langle P, x\rangle.\, \bigsqcap\{\mathcal{M}_{\mathit{Conditions}}(c, x), \mathcal{M}_{\mathit{Licensees}}(z, \lambda p.\, m(p)(P, x))\}\rangle$

Figure 19. KeyNote instantiation